Unique Patient Identifiers - why and for what?

Roderick Neame, BA,MA,PhD,MB,BChir
RoddyNeame@hic-ltd.com
Senior Lecturer, Kent Institute of Medicine and Health Sciences
University of Kent at Canterbury, Canterbury CT2 7NR, UK
and
Managing Director, Health Information Consulting Ltd,
Homestall House, Homestall Lane, Faversham ME13 8UT, UK
http://www.hic-ltd.com

Introduction

When an individual buys a service from a business – for example a meal in a restaurant, or a car service in a garage - he/she gathers information about the quality of the services supplied by the businesses, selects a service provider and makes a contract in which terms of payment are agreed. The services are provided, the payment is made and whatever business records may be considered necessary for warranty, accounting and the protection of either party against litigation will be kept. There is not normally any expectation that the individual will identify him/her self uniquely to the proprietor in the context of this transaction. One can argue that the arrangements pertaining to the provision of healthcare services should be no different.

The situation becomes a little more complicated where the arrangements for payment involve a third party who is not present at the time (eg credit provider, insurer). Then there will need to be some sort of certification that the credit of the consumer is 'good', and some summary of the services provided in this encounter, endorsed by both parties, which can be used to support the claim for payment, regardless of whether the claim comes from the provider or the consumer. More often than not this is the case in large parts of the world, whether the services in question relate to healthcare or any other form of business, and again one can argue that healthcare should be no different.

Healthcare has two special additional dimensions relating to the consumer individually and to the community generally. On an individual level two issues are significant. First the individual is likely to have relevant previous medical history, warnings, medications, problems and care: their health needs can only be best served if the service provider has full knowledge of that history. In other words it may be necessary for the consumer to be able to provide an index of past medical history and prove that they 'own' these events for the provider to offer them the best possible care in their particular situation. Second in the event that subsequent research identifies a risk associated with a particular service (eg prosthesis failure) the consumer may wish a record to be kept so that they can be warned if this risk might apply to them.

At a community level again two issues are significant. First is the situation where an individual may have a 'notifiable' disease for which statutory reports are required (eg tuberculosis, salmonella) for the protection of the community: it may be necessary to identify the individual in order to ensure that the records are accurate and actions which follow are appropriately directed. Second the individual may have a condition for which the best quality treatment

Correspondence to:
Homestall House, Homestall Lane, Faversham, Kent ME13 8UT, UK
Email roddyneame@hic-ltd.com; fax: +44 (0)870 6727176; tel: +44 (0)1795 538390
WWW: http://www.hic-ltd.com

practice is unknown, and this probably applies to the majority of illness at the present time. The entire community has a legitimate interest in collecting synopses of care to compile information on what treatments are and are not effective. However in these cases the actual identity of the individual is not required, as long as it is possible to link together care events for that same individual into a sequence, and to have some (limited) classifications for the individual (eg age range, sex, domicile region etc).

Therefore when a patient attends a care service provider there are fundamentally two groups of issues that the provider must consider (one may argue about the order of priority):

- **clinical**: other than the information that can be provided by the patient, what further information is required from whom/where in order to deliver appropriate (high quality, low risk, cost-effective) preventive and curative care to this individual that integrates with any other relevant wellness and illness programs involving the same individual; what clinical records need to be kept to inform others of the event (subject to privacy constraints) and/or for statistical analysis and research
- **business**: who will be paying for the services involved in providing care, how much, (and with what delay); if the payer is a third party, what data must be collected to substantiate the claim for services provided to this patient; what additional records of the transaction must be kept in case of litigation

Fundamentally this identifies the twin requirements which a unique patient identifier (UPI) for health purposes should be required to support. A clinician may argue that the clinical issues are all that matters, and administrator may argue the same for business needs: both are legitimate requirements that a UPI must be able to support. Ultimately the purpose of any healthcare system is the provision of quality care services to the individual: this cannot be undertaken in isolation from the real business issues of who is to pay, although it is up to the patient him/herself to make arrangements regarding payments. The fact that a patient may (or may not) be entitled to recover some or all of those costs from a third party is not directly related to the provision of care itself, but may indirectly influence what is done as well as the records that are made.

Patient Identifiers and their use

The majority of health care systems make use of patient identifiers, each of which is intended to be unique within its own particular jurisdiction or domain of use. In practice many jurisdictions are very limited in size at the present time - for example a single provider or hospital. Furthermore most ‘systems’ for issuing such identifiers are poorly formalised and often poorly managed such that **duplication** (one patient, multiple identifiers) is common, and **sharing** (multiple patients, one identifier) is not uncommon. For example in many primary care clinics the receptionist ‘uniquely identifies’ a new patient often based on some derivative of the first few letters of the family name. This is quite sufficient for their local clinical and business needs, but of limited use to anyone else or for automated management since the number of individuals in a district with the family name 'Smith' or 'Jones' (or 'Wing' or 'Mohammed' in different global regions) is likely to be large. Most hospitals issue the next number in sequence from their master index system, very often without adequate checking as to whether the individual has previously been registered, so resulting in multiple duplicate entries and therefore fragmented care records. Many hospitals run several departmental systems, each with their own master index, so resulting in further fragmentation, which serves the needs of the patient poorly, and is of little value as a UPI.

What is a Unique Identifier?

Reflect for a moment - what is a UPI? A UPI is just another name for an entity, such as an individual. It is a code, in just the same way as every care service and clinical diagnosis has another code-form name (eg coding systems such as Read, ICD, DRG, CPT, MBS etc). Why use a code? Because a code:

- eliminates ambiguity - eg synonyms, alternate names, spellings etc
- can easily be represented for automated handling - eg bar code, on a magnetic stripe
- is optimised for electronic exchanges - compact, fixed length etc
- can be validated and self-checking - eg with a check digit to ensure correct entry
- can be 'understood' by a computer - for analysis, searching, sorting, indexing etc

But there is no reason whatever why an individual should be limited to just one UPI: they may have many. The key is to be able to link them together where necessary, to recognise that all these UPIs belong to the same person, with their associated records. Whether this is achieved through the adoption of a single 'master' UPI, or through a 'mapping table' that cross-links all these alternates is another issue: the technology to do either or both exists.

UPI Design Principles

If we create the situation where all individuals are uniquely identified, if only for the purposes of receiving and paying for healthcare services, it raises anxieties about the increased potential for infringement of basic human rights, such as the right to privacy of personal information. There is a general acceptance that individuals should have the right to control who knows what about them in some domains, and to expect that information exchanged in confidence in the context of one purpose (such as the receiving of healthcare services) should not be divulged for any other purpose without the express permission of the parties. This expectation is enshrined in various pieces of legislation, with rather variable integrity, enforceability and impact on 'normal' practices within that jurisdiction.

In this context the design principles for UPIs in health raise several key issues. Should the UPI be designed to constitute a legal identification? Should it be designed to reveal something about the holder, or simply be a random (possibly self-checking) code? And should it be designed for cross-linking with identifiers in other government/business sectors?

UPIs and legal Identity. A UPI is required (1) in order to keep track and prove ownership of personal health records, (2) to certify entitlement to third party payment benefits from one or more sources, and (3) on occasion to identify an individual for statutory purposes (eg in relation to notifiable diseases). The first aim requires no proof of identity other than to confirm that all the events belong to the same person. The second aim has two aspects: where a private insurance arrangement has been made there is no need for the individual to prove their identity, merely to confirm that they are the insured. But where an individual wishes to assert their entitlement to public money, they will need to demonstrate to the relevant authority that they are so entitled, and this may involve proof of identity. The third aim clearly requires proof of identity. If all these purposes are to be served by a single identifier, then it must be based on some proof of legal identity - but there is no need for these different purposes to be served by a single UPI: an individual may have several different identifiers for different purposes.

UPIs and the holder. The UPI is simply a code, an alternate name for the holder. The only reasons why a UPI might be required to reveal something about its holder would be to prevent fraudulent use of the UPI, for example to gain access to encounter records or to payment benefits to which the holder was not entitled. The argument that the UPI should reveal something about its holder seems therefore to be irrelevant: the real issue is for the holder to be able to authenticate in some simple way that the UPI belongs to them. The normal techniques

for this are based on (1) something one holds (eg a UPI card), (2) something one knows (eg a password or code) and if needed (3) something unique to oneself (eg fingerprint, iris scan or other biometric identifier). There is no need for the UPI itself to reveal anything about the holder.

UPIs and Cross-links to other sectors. The subject of this article is a UPI for healthcare. Other than as indicated above, healthcare is an intensely personal issue and should be treated in complete isolation from any other facet of one's physical existence. There is, therefore, no valid reason to develop a UPI system which enables data matching exercises to be carried out across sectors, or which makes the establishment of such links easy. However by its very nature a UPI for health is likely to match up one-for-one with a UPI for any other sector: preventing abuse of that opportunity is one key purpose for a Privacy or Human Rights Commissioner within a jurisdiction – as, for example, in Australia and New Zealand

How would we wish to be able to use a UPI

Let us assume for the moment that a UPI system has been adopted for a jurisdiction (eg a Province or State), and that it has been issued to the individuals in some physical form. What would be its use? Consider a scenario.

Scenario: *A patient walks into a GPs surgery and requests an urgent appointment. She presents her UPI to the receptionist, who uses it to upload the details to which it permits access, which include patient name, address and date of birth; insurer, validity and insurance plan. The patient enters the doctor's office, and he uses her UPI to retrieve available clinical records.*

The clinic needs to register the patient on their system, to find any other relevant medical information, and to know to whom the bills are to be sent.

From a ***business*** perspective they need to know:

1. ***Authentication****: Is the patient the same person to whom the UPI was issued?*
2. ***Current Data****: Is the address and other administrative data current?*
3. ***Payer Validation****: Is the payer authorisation/insurance valid?*
4. ***Accountability and audit****: What data does the payer/insurer require in order to be able to process a claim for this event?*

From a ***clinical*** perspective the care provider needs to know:

5. ***Clinical Links****: Is there relevant medical history; if so, where and how can it be found?*
6. ***Care Plan****: Is any follow-up or preventive care due (eg immunisations, screenings) etc?*

Simply having a UPI does not necessarily solve any of these problems, although it may point in the right direction. There is a need for more than just a UPI. Consider the issues in turn.

1. **Authentication**. There are several ways of addressing this as noted above, for example the use of a PIN (as in the banking system), or a photo ID (as on driving licences) or the use of some biometric identifier such a thumbprint or iris scan. Whilst a PIN or password can be shared with another person to defraud the system, the other biometric authenticators are less easily subverted.

2. **Current Data**. Unless the data is updated dynamically through frequent use it will soon become an historic rather than a current datastore. When the UPI is used, data can be checked (eg current address) and updates communicated centrally to the UPI issuer electronically. Alternatively the patient can be put in control of their own data with a utility that allows them

to read and update some (or all) of the data held about them. Such utilities can be made available over the World Wide Web, or in public places such as libraries, hospitals etc, with automatic central updating capability. The growing interest in one's own health suggests that this would be attractive to many of the community.

3. **Payer validity**. Unless the UPI is used in conjunction with paying of insurance subscriptions, and the end of insurance validity date updated then, these data will be out-of-date almost from the time of issue. A simple on-line check with the insurer/payer of current details/validity can readily be undertaken: alternatively the UPI can be set up more along the lines of a credit card, with a credit limit approved by the issuer (who could be a bank). The provider need then only check with the issuer that sufficient credit exists to cover the costs. This has attractions to the financial community.

4. **Accountability**. One aspect of fraud is claiming for events that never took place; another is claiming for more services than took place in the event. The patient UPI could be used to generate an electronic statement that an event occurred with a particular provider (identified by his/her UPI) at a specific date and time, and sent for validation by a central event identifier system which assigns a unique event number and date/time. This could be forwarded to the insurer. While this says nothing about what happened, it does confirm that an encounter occurred, and it could permit the insurer easily and quickly to carry out a random audit, based on the electronic event statement, to ascertain the details.

5. **Clinical Linkages.** One option would be to create a central file for each individual on a network server: the authenticated UPI would permit access to that file and from it the provider can get a summary and further details of previous care events. However holding centralised databases of this type is comfortable neither to the community nor to the network manager. But there is an alternative, if a token is used (eg a smart card). In this instance the card can carry a synopsis of significant past care events, identifying who (doctor), where (place, organisation), when (date), what (problem, diagnosis, treatment). If further details are required they can be obtained from that source, or from a secure network repository.

6. Care Plan. The need for this is to minimise the 'falling through the gaps' problem that is so prevalent worldwide - anyone could have taken ownership of the individual's health care plan needs, but no-one actually does so. One option is the centralised database (outlined above) comprising a 'cradle to grave' record and which could carry a proactive care plan of immunisations, check-ups, screenings, recalls etc for the individual, so that anyone seeing that patient could do whatever was due. The other option is to commit that data to a card-based record (as above).

Implications for the UPI

Based on the above the UPI should:

- Be computer readable from a token, and internally validated (eg by check digit)
- Be capable of direct authentication, eg by PIN, password, biometric identifier
- Be used routinely so that the contents are kept up to date by sending updates from user workstations, and with the option for updates of selected parts of the associated data by the holder.
- Support on-line validation of payer/insurer details, contracts, terms, exclusions etc.
- Carry (or provide access to a centralised) synopsis of past care events (problems, medications, requests and results etc), preferably able to link on-line to further details of selected care events
- Carry (or provide access to a centralised) personal pro-active care plan

- Support central authentication that a care event with a specified provider occurred at a specified date/time, and provide an audit trail/link to that event.

The UPI should NOT:

- Be used or made available for purposes other than the provision of and payment for health services
- Be linked to other sectors (eg immigration, taxation etc)
- Be attached to care event reports collected for statistical analysis, except to identify where reports refer to the same (anonymous) individual to support longitudinal analyses
- Act as a legal identifier, except in so far as may be required to establish (1) right to public money subsidy for healthcare services and (2) identity for the purposes of statutory health-related legislation (although these could be managed using some other identifier)
- Of itself offer any insight into personal details or circumstances of the holder (eg through its intrinsic structure)

The UPI central Database

A UPI central database has two distinct elements: the UPI code itself, which will be associated with a name and address of the holder; and some additional data (such as date of birth, purchaser, possibly clinical data too). It's sensitivity from an information privacy perspective depends upon what it holds, how it is accessible and to whom. The mere existence of an individual is not normally considered a privacy issue. One can argue that the address and date of birth of an individual are essentially also in the public domain, but nevertheless this raises a privacy issue. The assembly of data into a new (computerised) format that makes these data more readily accessible and searchable is generally considered to be equivalent to the creation of new data and therefore constitutes a privacy issue.

What is beyond doubt is that any mechanism that makes possible the association of an identity with data that is not in the public domain, such as social security data, care purchaser arrangements, clinical records etc is definitively a privacy issue and a source of community concern if improperly handled. Consider the scenarios:

1. A user looks up clinical records (identified only by the UPI of the subject), finds those of particular interest; then looks up on the UPI database the identities of the subjects, together with their current addresses and sells the data to a medical appliance salesman, or alternatively sends blackmailing letters.
2. A researcher or statistical analysis technician finds a group of unusual or especially interesting event records and retrieves the identities of the individuals concerned to approach them for further study/survey
3. A claims processing clerk notices a claim for a termination of pregnancy relating to a close relative: once known, the information cannot subsequently become 'unknown' and it has a serious adverse social impact on their lives
4. An investigator is hired by an employer to check on the health of a potential key recruit: he enlists the assistance of a medical clerk who retrieves information indicating that the recruit has a high risk of developing a debilitating illness, and the matter is terminated.
5. A psychopath searches the UPI database for young unmarried females living alone, and uses this list to identify subjects for stalking and attacks.

There is clear evidence, at least in some countries, of organised operations to gather such information in the context of decisions regarding life insurance, mortgages, hire purchase,

employment and more, constituting a multi-million dollar industry based on systematic invasions of privacy. There are entire industries making a living out of assembling such data for their customers, and often not in the best interests of the subject.

Access to the UPI database should, therefore, be restricted to accredited users, with all appropriate security and audit trailing of accesses and changes. It must have proper rules governing access to it (eg use only where there is a duty of care relationship with the individual) which can be audited and for breach of which penalties are applied.

All users must be individually identifiable with authenticated identifiers, and the most appropriate technology for this at the present time would seem to be a smart ID card. Provision of a UPI token to patients would mean that the need to permit searches of the database would be greatly reduced, since each patient should be able uniquely to identify and authenticate themselves, as well as control access to any central record(s) relating to themselves.

However implementing a UPI system is itself of little value unless there is a commitment:

- **By the government/funders** to create a system, and especially a financial system, that supports and provides incentives for appropriate use of the UPI, and with dis-incentives for failing to use it (eg via the claims management process)
- **By the healthcare purchasers/insurers and providers** to implement an architecture and a **technology** that supports the exchange of information between record stores based on this UPI over the same area of usage
- **By individuals (both patients and providers**) to take full advantage of the opportunities and benefits provided by such technology when it is available and to use it consistently

Critical Issues

There are a number of key issues that remain before the full benefit of a UPI system can be realised. One of the essential purposes of a proper UPI system is to enable the sharing of clinical information in a patient-focussed way, but before that can happen freely some stumbling blocks must be removed. One must address the issues that at present make it unattractive to provider to share information with patients and other providers. This is tied up in issues of commercial advantage, seeking appropriate payment for providing quality information to others, concerns over professional privacy and law suits and the thorny problem of data ownership. There are pragmatic solutions to all these problems, which the author has developed, which will be outlined elsewhere.

Summary

This paper outlined what may be considered as the 'gold standard' for an effective UPI system in health. It argues that simply adopting a unique identifier achieves little unless it is implemented in a way that can support some or all of the core functions outlined above. There are dual business and clinical purposes for having a UPI system in place, but these can come into conflict with one another unless the issues are carefully separated and resolved. The functions that should be served by a UPI system are listed: it should be noted that few, if any, national health services have put in place a UPI system that brings significant clinical benefits to the patient, as is proposed here.

The paper also identifies that a UPI system presents risks to personal privacy, and makes some suggestions as to how these should be addressed, particularly through the use of smart cards, and the process of empowerment of patient to approve (or not) accesses to their personal data.